Hastings Law Journal

Volume 54 | Issue 4 Article 2

1-2003

Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law

Orin S. Kerr

Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law

by
ORIN S. KERR*

Introduction

Consider a typical computer crime investigation. A computer hacker hacks into the servers of an Internet commerce company looking for credit card numbers to copy and sell.[1] The company discovers the attack and contacts the FBI for assistance. The FBI opens an investigation and focuses its efforts on attempting to trace the evidence of the attack from the victim back to the hacker. The government's strategy will be to follow the trail of "electronic bread crumbs" that the attack may have left behind, such as connection logs and stored files, until they can trace back the attack and identify the wrongdoer. This process is highly regulated by federal electronic surveillance statutes that require the government to obtain court orders nearly every step of the way; the court orders compel the owners of the ISPs and other servers that may have records relating to the attack to divulge the information they have to the government.[2] Imagine that these methods prove successful, and provide information pointing to the hacker. At this point, the FBI obtains a search warrant authorizing law enforcement to search the hacker's home and seize his computer. FBI agents execute the warrant, and a search of the computer uncovers the stolen credit card numbers inside it. The FBI agents arrest the hacker.

---

* Associate Professor, George Washington University Law School. Thanks to Jim Dempsey, John Podesta, Paul Schwartz and Peter Swire for commenting on an earlier draft.

1. *See e.g.*, Patrick Collinson, *Cybercrime: Have Hackers Got Your Number?*, THE GUARDIAN (London), May 18, 2002, at P2; Thomas E. Weber, *E-World: Credit Fraud Online Hurts Merchants More Than Shoppers*, WALL. ST. J. (Europe), Dec. 10, 2001, at 10; Harvey Morris, *Teenage Hacker Admits Fraud*, FIN. TIMES (London), July 7, 2001, at 2.

2. *See infra* Part II.B.

Now imagine you are the hacker's defense attorney. You believe the government violated the rules that regulate criminal investigations in the course of investigating your client, and you want the trial court to suppress the evidence linking your client to the evidence. But how? Your most obvious option will be to rely on the Fourth Amendment's suppression remedy to challenge the search warrant at your client's home and the seizure and subsequent search of your client's computer. You can argue that the search warrant was not based on probable cause, was unconstitutionally overbroad, or that the search was executed in flagrant disregard of the warrant.[3] If you can overcome the formidable *Leon* good faith hurdle on review of the warrant,[4] the Court may suppress the evidence and dismiss the charges against your client.[5] But if you want to challenge the government's surveillance practices that led to the probable cause supporting the warrant, you will find yourself out of luck. Even assuming that law enforcement agents violated the statutory surveillance laws in the course of obtaining their court orders and compelling evidence from the ISPs, the government will argue that the Court should not even entertain the challenge because the laws lack a statutory suppression remedy.[6] Regardless of whether the government complied with the surveillance statutes, the government wins.

And the government will be right. While very generous civil remedies exist against violations of a maze of statutes that on paper offer significant privacy protection for Internet users, the statutory Internet surveillance laws lack a suppression remedy.[7] A defendant charged with a crime can sue the government for civil damages if the FBI violates the surveillance laws to catch him, and can sue ISPs and other third parties if they violated the surveillance laws as well, but he cannot rely on those violations as a basis for suppression of the evidence against him. While the telephone surveillance laws offer a

3. For a summary of the cases evaluating all three arguments in the context of search warrant to search and seize computers, *see* COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS ch. 2 (2002), *available at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm [hereinafter CCIPS MANUAL].

4. *See* United States v. Leon, 468 U.S. 897, 905 (1984).

5. *See, e.g.*, Taylor v. State, 54 S.W.2d 21, 27 (Tex. Crim. App. 2001) (reversing conviction of defendant for possession of child pornography obtained via the Internet on the grounds that the search warrant executed at the defendant's home was not based on probable cause).

6. *See, e.g.*, United States v. Kennedy, 81 F. Supp. 2d 1101–11 (D. Kan. 2000) (declining to suppress evidence obtained in violation of 18 U.S.C. § 2703 because Congress did not include a statutory suppression remedy under the statute).

7. *See infra* Part II.B where the current remedies scheme is explained in depth.

suppression remedy for at least some violations, the Internet surveillance laws do not.[8] Faced with this reality, a defense attorney is unlikely to raise statutory arguments in a motion to suppress. Instead, she will base the challenge solely on the constitutionality of the warrant executed at the defendant's house. The government's compliance with the Internet surveillance laws will remain unexamined.

This dynamic, repeated hundreds of times over, has had a dramatic and unfortunate impact on the law of Internet surveillance that has never before been acknowledged. Thanks to the absence of an exclusionary rule but the presence of strong civil provisions, the courts only rarely encounter challenges to Internet surveillance practices—and when they do, the challenges tend to be in civil cases between private parties that raise issues far removed from those that animated Congress to pass the statutes. As a result, the courts have not explained how the complex web of surveillance statutes apply in routine criminal cases, but instead have interpreted those statutes in unexpected civil contexts where the implications of the court's decision for the bulk of criminal cases tends to be unknown to the court and ignored by the parties. The dynamic has given the law of Internet surveillance a decidedly quirky flavor. The law remains unusually obscure, and the rare judicial decisions construing the statutes tend to confuse the issues, not clarify them. Internet surveillance law remains a fog, and the remedies Congress has chosen deserve much of the blame.

This Article argues that Congress should restructure the remedies scheme of Internet surveillance law by adding a statutory suppression remedy for violations of the Internet surveillance statutes. Such a change would benefit both civil libertarian and law enforcement interests alike. On the civil libertarian side, a suppression remedy would considerably increase judicial scrutiny of the government's Internet surveillance practices in criminal cases. The resulting judicial opinions would clarify the rules that the government must follow, serving the public interest of greater transparency. Less obviously, the change could also benefit law enforcement by altering the type and nature of the disputes over the Internet surveillance laws that courts encounter. Prosecutors would

8. The statutory line is not technically between a telephone and the Internet, but rather communications that contain the human voice and those that do not. *Compare* 18 U.S.C. § 2510(1) (Supp. 2002) (defining wire communications), *with id.* § 2510(12) (defining electronic communications). For the most part, this statutory distinction tracks the difference between telephone and Internet communications. Telephone calls ordinarily carry the human voice, and Internet communications do not, although there are cases in which the opposite is true. For the sake of simplicity, however, I will refer to the difference as one between Internet and telephone communications.

have greater control over the types of cases the courts decided, enjoy more sympathetic facts, and have a better opportunity to explain and defend law enforcement interests before the courts. The statutory law of Internet surveillance would become more like the Fourth Amendment law: a source of vital and enforceable rights that every criminal defendant can invoke, governed by relatively clear standards that by and large respect law enforcement needs and attempt to strike a balance between those needs and privacy interests.

Importantly, my argument bypasses the usual debate over the merits of suppression remedies and the exclusionary rule. The usual debate focuses on the enforceability of legal rules.[9] Is the threat of losing important evidence needed to deter the police from violating the law? This is an important debate, and I confess an attraction to the exclusionary rule in part because it places the right incentives on law enforcement to follow the rules.[10] In the specific context of Internet surveillance law, however, the enforceability debate carries less force given the reality of how Internet crime investigations work.[11] Unlike traditional criminal investigations, Internet crime investigations are conducted pursuant to court orders via the

9. *See Leon*, 468 U.S. at 906–09 (discussing the debate over the scope of the Fourth Amendment exclusionary rule in terms of its deterrent effect); Devon W. Carbado, *(E)Racing the Fourth Amendment*, 100 MICH. L. REV. 1006, 1006–07 (2002) ("The most commonly invoked rationale for the exclusionary rule is deterrence. The argument is that police are less likely to engage in unconstitutional searches and seizures if they know that evidence acquired in violation of a person's constitutional rights will be inadmissible at trial."); L. Timothy Perrin et al., *If It's Broken, Fix It: Moving Beyond the Exclusionary Rule: A New and Extensive Empirical Study of the Exclusionary Rule and a Call for a Civil Administrative Remedy to Partially Replace the Rule*, 83 IOWA L. REV. 669 (1998); Myron W. Orfield, Jr., Comment, *The Exclusionary Rule and Deterrence: An Empirical Study of Chicago Narcotics Officers*, 54 U. CHI. L. REV. 1016, 1019–22 (1987); William C. Heffernan & Richard W. Lovely, *Evaluating the Fourth Amendment Exclusionary Rule: The Problem of Police Compliance with the Law*, 24 U. MICH. J. L. REFORM. 311, 319–21 (1991); Comment, *Effect of Mapp v. Ohio on Police Search-and-Seizure Practices in Narcotics Cases*, 4 COLUM. J. L. & SOC. PROBS. 87 (1968).

10. In my relatively brief time as a prosecutor, I noticed that agents and police officers can occasionally see legal niceties as impediments to their efforts to protect public safety by identifying and arresting criminals, leading to their convictions in court. When a suppression remedy is in place, the lawyer's goal of following the law comes into alignment with the police officer's goal of building a provable case against the suspect. Following the law becomes the most effective way for a police officer to do his or her job.

11. For examples of how the enforceability debate has dominated discussions of whether the Internet surveillance laws should include a statutory suppression remedy, *see, e.g.*, Michael S. Leib, *E-mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III's Statutory Exclusionary Rule and Expressly Reject A "Good Faith" Exception*, 34 HARV. J. ON LEGIS. 393, 418–19, 437–38 (1997); Peter J. Georgiton, Note, *The FBI's Carnivore: How Federal Agents May Be Viewing Your Personal E-Mail And Why There Is Nothing You Can Do About It*, 62 OHIO ST. L. J. 1831, 1866 (2001) ("Without a suppression remedy, the FBI has no real incentive to ensure that they are following the protections Congress established with Title III and the ECPA.").

intermediaries of ISPs and other third parties, who demand court orders from the government and typically make sure that the I's are dotted and T's are crossed before they will comply with them.[12] Further, for a range of reasons, Internet crime investigations are mostly conducted by federal investigators,[13] who are carefully trained and closely watched by the federal prosecutors who must sign the applications for court orders.[14] In this environment, traditional concerns about rogue police officers may retain their rhetorical force, but fortunately seem less attuned to the mechanics of Internet crime investigations than those of traditional criminal investigations. The existence of a suppression remedy may have a marginal effect on the government's incentives to comply with the statutory scheme, but that effect is likely to be quite small.

I think the real issue raised by remedies for violations of Internet surveillance laws relates less to the enforcement of the law than its clarity and shape. A suppression remedy would change Internet surveillance law considerably. It would clarify the law, inform the public, and influence the law's doctrinal development. I will develop this argument in the following three sections. Section I, explains the importance of the statutory remedy Congress chooses, and why statutory rather than constitutional rights and remedies play a primary role in regulating Internet crime investigations. Section II argues that the current remedies scheme has impeded the natural development of Internet surveillance law. As a direct result of the

12. *See* How Far Will the Feds Go to Push Favorable Surveillance Laws?, E-Commerce Law Week (Sept. 7, 2002), *at* http://www.steptoe.com (advising ISPs to "undertake an independent evaluation of the order's lawfulness rather than simply relying on DOJ's interpretation of the law" when confronted with a court order to conduct surveillance).

13. Computer crimes tend to be investigated at the federal level rather than the state level for a host of reasons. First, the national and even international nature of the evidence collection process poses special challenges for states. Second, federal law creates a floor but not a ceiling for state Internet surveillance practices, and both imposes special burdens on state surveillance laws and allows the states to impose even greater burdens. Third, state surveillance practices can be burdened relative to federal practices by expansive interpretations of state equivalents of the Fourth Amendment, which govern state agents but not federal agents. *See generally* ORIN S. KERR, COMPUTER CRIME: CASES AND MATERIALS ch. 10 (forthcoming 2005).

14. *See* 18 U.S.C. § 2516(3) (1993) (requiring that an application for a Wiretap Order to intercept electronic communications must be signed by an "attorney for the Government"); *id.* § 3122(a)(1) (requiring that an application for a Pen Register Order must be signed by an "attorney for the Government"). In the case of a court order to compel an ISP to disclose stored evidence under the Stored Communications Act pursuant to *id.* § 2703(d) (Supp. 2002), a "government entity" must apply for the order, but the application need not be signed by an attorney. *Id.* In most cases, however, the applications are in fact signed by a government attorney such as an Assistant U.S. Attorney involved in the investigation.

remedies scheme Congress has chosen, courts have not answered how the statutes apply to routine criminal cases but instead have applied the statutes in quirky civil contexts which have led to more confusion, rather than less. Finally, in Section III, I propose that Congress should add a statutory suppression remedy to the Internet surveillance statutes, and offer reasons why both civil liberties groups and law enforcement should support the proposal.

I. The Rights and Remedies of Internet Surveillance Law

To understand the importance of statutory remedies within Internet surveillance law, it is essential to understand the differences between the laws that regulate criminal investigations in the physical world and the laws that regulate Internet crime investigations. In the former, the Fourth Amendment acts as the primary guide; in the latter, statutory surveillance laws do. To a large extent, Internet surveillance law is statutory law, and the remedies of Internet surveillance law are statutory remedies. This section begins by explaining the traditional rules and remedies that govern physical-world crime investigations and next explains why those same rules generally do not govern Internet crime investigations. The section then contrasts the traditional constitutional regime with the statutory rules that govern Internet crime investigations, focusing on the significant differences between the suppression remedies traditionally available in constitutional cases and the civil remedies currently available in the statutory context of Internet surveillance.

A. The Traditional Framework: Constitutional Protections and Exclusionary Remedies

In the physical world, the Fourth Amendment acts as the primary regulator of law enforcement conduct in the course of criminal investigations. Fourth Amendment rules apply to federal, state, and local investigators,[15] and tell the police what they can and cannot do as they gather evidence of crime. Although the Fourth Amendment insists on an overarching constitutional goal of reasonableness,[16] the Supreme Court has enforced that goal by creating highly specific rules that govern in remarkable detail what the police can do, when, and under what circumstances.[17]

15. *See* Mapp v. Ohio, 367 U.S. 643 (1961) (holding that the exclusionary rule of the Fourth Amendment applies to the states through the Fourteenth Amendment).

16. *See* Illinois v. McArthur, 531 U.S. 326, 330 (2001) (noting that the Fourth Amendment's "central requirement is one of reasonableness").

17. *See id.* ("In order to enforce that requirement [of reasonableness], this Court has interpreted the Amendment as establishing rules and presumptions designed to control conduct of law enforcement officers . . . ."); Ronald J. Allen. & Ross M. Rosenberg, *The*

To simplify dramatically, the Fourth Amendment allows law enforcement to go freely into public spaces that are not protected by a "reasonable expectation of privacy,"[18] but generally requires a search warrant or special factual circumstances for the government to go into private spaces that *are* protected by a reasonable expectation of privacy.[19] As a practical matter, this approach carves out private spaces where law enforcement can't ordinarily go without a warrant, and separates them from public spaces where it can. If government surveillance does not implicate a reasonable expectation of privacy, law enforcement ordinarily remains free to conduct it. When surveillance does implicate such privacy interests, the police may need "reasonable suspicion" of criminal activity to take certain investigative steps,[20] probable cause to take others,[21] and generally must obtain a search warrant from a neutral magistrate before executing the most invasive forms of surveillance.[22]

The exclusionary rule provides the primary means of enforcing the Fourth Amendment. If the police break the rules and violate a defendant's Fourth Amendment rights in the course of an investigation, the defendant can move for suppression of the evidence obtained,[23] and any fruits following from it.[24] Suppression is not an automatic remedy if the police violate the Fourth Amendment.[25] Courts will not suppress evidence obtained from a violation of the rights of someone other than the defendant.[26] The police can also use evidence obtained from the execution of a defective search warrant if they relied in good faith on the warrant.[27] In most cases, however, a court must suppress the evidence obtained in violation of the defendant's Fourth Amendment's rights.

Fourth Amendment and the Limits of Theory: Local Versus General Theoretical Knowledge, 72 ST. JOHN'S L. REV. 1149 (1998).

18. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 450 (1989) (allowing law enforcement to pilot helicopter that allowed them to view the defendant's property and observe it from public airspace without a warrant).

19. *See, e.g.*, Kirk v. Louisiana, 536 U.S. 635 (2002) (holding that absent exigent circumstances, the police may not enter a suspect's home without his consent or the consent of someone with common authority over the area entered).

20. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 27 (1968) (reasonable suspicion needed to stop a suspect for questioning).

21. *See, e.g.*, Delaware v. Prouse, 440 U.S. 648, 659, 660 (1979) (probable cause to believe traffic violation occurred justifies decision to stop an automobile).

22. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001) (search warrant needed to direct thermal imager in the direction of a suspect's home).

23. *See Mapp*, 367 U.S. at 655 (holding that the exclusionary rule of the Fourth Amendment applies to the states through the Fourteenth Amendment).

24. *See* Wong Sun v. United States, 371 U.S. 471, 487–88 (1963).

25. *See supra* notes 6–11 and associated text.

26. *See* Rakas v. Illinois, 439 U.S. 128, 143 (1978).

27. *See Leon*, 468 U.S. at 905.

Defendants also have civil remedies for Fourth Amendment violations, although these remedies have played a decidedly secondary role in the development of the Fourth Amendment. In a federal investigation, a defendant can bring a *Bivens* action against the government for money damages,[28] and in a state investigation, a defendant can sue the state under 42 U.S.C. § 1983.[29] Few criminal defendants bother to sue, however. Unsurprisingly, most defendants care more about staying out of jail than about bringing a lawsuit against the government for money damages. As a result, the number of Fourth Amendment decisions arising from motions to suppress dwarfs the number arising from civil actions against the government.

B. Internet Surveillance Law and the Shift from Constitutional to Statutory Protections

The source of Internet surveillance law differs considerably from that of traditional search and seizure law. In physical-world investigations, the governing rules usually derive from the Fourth Amendment. In the Internet context, however, the governing standards of law are primarily statutory.[30] This may change in the future, as the law is uncertain; many basic questions about the scope of constitutional protections remain. Today, however, it is fair to say that Internet privacy is primarily statutory privacy, and the remedies that govern Internet privacy are primarily statutory remedies.

To see why statutory rather than constitutional protections provide the essential rules governing Internet surveillance law, it helps to compare what the Fourth Amendment protects with how the Internet works. Recall that the Fourth Amendment effectively carves out private spaces where law enforcement can't ordinarily go without a warrant and separates them from public spaces where it can. One important corollary of this structure is that when a person sends out property or information from her private space into a public space, the exposure to the public space generally eliminates the Fourth

28. *See* Bivens v. Six Unknown Named Agents of Bureau of Fed. Narcotics, 403 U.S. 388, 388 (1971).

29. Section 1983 provides:

> Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress, except that in any action brought against a judicial officer for an act or omission taken in such officer's judicial capacity, injunctive relief shall not be granted unless a declaratory decree was violated or declaratory relief was unavailable.

30. I develop this argument in Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 627–30 (2003).

Amendment protection. If you put your trash bags out on the public street,[31] or leave your private documents in a public park,[32] the police can inspect them without any Fourth Amendment restrictions.

The Supreme Court's cases interpreting this so-called "disclosure principle" have indicated that the principle is surprisingly broad. For example, the exposure need not be to the public. Merely sharing the information or property with another person allows the government to go to that person to obtain it without Fourth Amendment protection. If you tell a secret to your friend,[33] or give a document to your accountant,[34] the Fourth Amendment will not offer protections from police efforts to get the secret from your friend or the document from your accountant. Even more broadly, the disclosure need not be to a human being. In *Smith v. Maryland*,[35] the Supreme Court concluded that the same principle applies when a person enters information into another person's machine. By telling the machine your private information, the Supreme Court held, you relinquish an expectation of privacy in the information just as you would if you had told your private information to a person.[36]

Why does this matter to Internet surveillance? It matters because the basic design of the Internet harnesses the disclosure, sharing, and exposure of information to many machines connected to the network. The Internet seems almost custom-designed to frustrate claims of broad Fourth Amendment protection: the Fourth Amendment does not protect information that has been disclosed to third-parties, and the Internet works by disclosing information to third-parties. Consider what happens when an Internet user sends an e-mail.[37] By pressing "send" on the user's e-mail program, the user sends the message to her ISP, disclosing it to the ISP, with instructions to deliver it to the destination. The ISP computer looks at the e-mail, copies it, and then sends a copy across the Internet where it is seen by many other computers before it reaches the recipient's ISP. The copy sits on the ISP's server until the recipient requests the e-mail; at that point, the ISP runs off a copy and sends it

31. California v. Greenwood, 486 U.S. 35, 40–41 (1988).

32. United States v. Procopio, 88 F.3d 21, 26–27 (1st Cir. 1996).

33. *See* Hoffa v. United States, 385 U.S. 293, 302 (1966).

34. *See* United States v. Miller, 425 U.S. 435, 443 (1976).

35. 442 U.S. 735 (1979).

36. *See id.* at 744–45 (viewing disclosure to a machine as identical to an analogous disclosure to a person in the context of a pen register, and concluding that for reasons of coherence the Court would not apply a separate rule simply because the company "decided to automate").

37. *See* PRESTON GRALLA, HOW THE INTERNET WORKS 87 (2001).

to the recipient.[38] While the e-mail may seem like a postal mail, it is sent more like a post card, exposed during the course of delivery.[39]

Does this mean that the Fourth Amendment offers no protection to Internet communications? It's too early to tell. Courts may follow the logic of this syllogism, or they may not.[40] However, courts have already indicated that defendants do not retain Fourth Amendment protection in non-content information such as basic subscriber information.[41] Courts have also declined to find Fourth Amendment protection in the contents of computer usage in the few fairly specific situations that have been litigated.[42] At least as of the time of this writing, the answer to the question of how much privacy protection the Fourth Amendment guarantees to Internet communications appears to be "not much." And certainly not enough.

Fortunately, Congress understood these difficulties at a remarkably early date, and passed legislation to protect Internet privacy long before most Americans had even heard of the Internet.[43] The important date is 1986, when Congress amended the 1968 Wiretap Act by passing the Electronic Communications Privacy Act ("ECPA").[44] ECPA created a comprehensive set of statutory protections that give roughly the protections against Internet surveillance that the Fourth Amendment might have protected absent the disclosure principle. Although ECPA has been amended many times since 1986, the 1986 Act set the basic framework of Internet surveillance law: all subsequent changes have merely nibbled around the edges of the law that Congress passed with tremendous foresight back in 1986.

38. *See id.*

39. *See* SIMSON GARFINKEL, PGP: PRETTY GOOD PRIVACY 8–9 (1995).

40. *See*, e.g., *United States v. Bach*, 310 F.3d 1063, 1066 (8th Cir. 2002) (assuming, but not deciding, that the holder of a Yahoo! Internet account retains a reasonable expectation of privacy in the contents of files stored in the account, but noting the uncertainty of whether in fact it does.). *See also* Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 57, 365–67 (2003) (discussing different ways in which courts might approach whether the Fourth Amendment protects remotely stored computer files).

41. *See* Guest v. Leis, 255 F.3d 325, 335–36 (6th Cir. 2001) (finding no expectation of privacy in non-content information disclosed to ISP); United States v. Hambrick, 55 F. Supp. 2d 504, 508–09 (W.D. Va. 1999), *aff'd* 225 F.3d 656 (4th Cir. 2000) (unpublished opinion); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (unpublished opinion).

42. *See Leis*, 225 F.3d at 333; United States v. Butler, 151 F. Supp. 2d 82 (D. Me. 2001); United States v. Simons, 206 F.3d 392 (4th Cir. 2000). *But see* United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996).

43. The word "Internet" was coined in 1982. Timeline: Evolution of the Internet, Table 1, http://www.eatonhand.com/thues/wtable01.htm (last visited Feb. 2, 2003).

44. Pub.L. 99-508 (codified as amended at 18 U.S.C. § 2510 (1986)).

The framework of electronic surveillance laws created by ECPA consists of three statutes: the Wiretap Act,[45] the Pen Register statute,[46] and the Stored Communications Act.[47] The Wiretap Act and the Pen Register statute both regulate access to prospective, real-time Internet communications.[48] The Wiretap Act regulates access to "contents" of communications such as e-mails, and the Pen Register statute regulates access to non-content information, "dialing, routing, addressing, and signaling information," such as the originating e-mail addresses in an e-mail inbox. Both the Wiretap Act and the Pen Register operate in the same basic way. They each enact general criminal prohibitions on both government and non-government access to communications but permit a few specific exceptions to allow such access.[49] One of those exceptions allows the government to obtain a court order to either access the communications directly or order an ISP to access the communications on the government's behalf.[50] In the case of the Wiretap Act, the court order is quite difficult to obtain. The government must obtain a "super warrant" to access the actual contents of communications, which is the highest threshold court order in American criminal law.[51] In contrast, the Pen Register order is quite easy for the government to obtain. To access non-content information, the lawyer for the government must merely apply to the court and certify that the information likely to be obtained is relevant to an ongoing criminal investigation.[52]

While the Wiretap Act and Pen Register statute regulate access to communications in transit, the Stored Communications Act regulates government access to both the contents and non-contents of stored communications.[53] The Act works by regulating the government's interactions with third-party providers such as ISPs and other servers that store communications on behalf of its users and subscribers. While the Fourth Amendment apparently places few if any restrictions on government access to communications held by

45. 18 U.S.C. §§ 2511–22.

46. 18 U.S.C. §§ 3121–27.

47. 18 U.S.C. §§ 2701–11.

48. *See* CCIPS Manual, *supra* note 3 at ch. 4.

49. *See* 18 U.S.C. § 2511 (1993 & Supp. 2002) (Wiretap Act); *id.* § 3121 (Pen Register statute).

50. *See id.* § 2516 (Wiretap Act); *id.* § 3123 (Pen Register statute).

51. *See id.* § 2518 (explaining steps the government must take to satisfy legal requirements needed to obtain a Wiretap Order).

52. *See id.* § 3123 (explaining steps the government must make to satisfy legal requirements needed to obtain a Pen Register Order).

53. Put another way, the Stored Communications Act regulates retrospective surveillance, allowing the government to access communications that are already stored and existing, rather than prospective surveillance of communications not yet sent. *See* Kerr, *supra* note 30, at 616–18.

ISPs, the Stored Communications Act does. The statute harnesses a client/server model, and gives clients (described as "customer[s]" or "subscriber[s]") rights in their records held by the server (the "provider" of the "service"[54]). Under the Act, the government must obtain a subpoena to compel ISPs to divulge certain information; must obtain a "specific and articulable facts" court order to compel an ISP to divulge other information; and must obtain a probable cause search warrant to compel an ISP to divulge the most private information, such as the contents of unopened e-mails in a user's inbox.[55] The Act also places limits on the ability of ISPs to disclose information relating to a user: while the Fourth Amendment places no limits on such disclosure, the Stored Communications Act forbids ISPs from disclosing information to the government except in specific situations.[56]

Taken together, these three statutes create a set of privacy protections that is roughly analogous to the privacy protections that the Fourth Amendment offers in the physical world. In some ways, the privacy protections offered by the statutory rules exceed those offered by constitutional standards;[57] in other ways, the statutory protections fall considerably short of the traditional rules.[58] But the key point for our purposes is that the Supreme Court's interpretation of the Fourth Amendment has led Congress to enact Fourth Amendment-like rules by statute. This means that when the government violates the rules governing electronic surveillance, the violations tend to be statutory, and the remedies are up to Congress, rather than the Constitution.

54. 18 U.S.C. § 2702 (1993); *id.* § 2703. The terms "customer" and "subscriber" are not defined by the statute.

55. *See id.* § 2703; CCIPS Manual, *supra* note 3, ch 3.

56. *See* 18 U.S.C. § 2702; CCIPS Manual, *supra* note 3, ch 3.

57. For example, the statutes all offer protection against both government access *and* access to information by private actors.

58. For example, 18 U.S.C. § 2703(b) allows the government to obtain access to stored opened e-mails without a search warrant. Focusing on these relative weaknesses in the surveillance statutes, Professor Solove writes:

> The current statutory regime that has attempted to fill the void created by the judicial evisceration of the Fourth Amendment is inadequate because it results in the de facto watering down of the warrant and probable cause requirements of the Fourth Amendment. As warrants supported by probable cause are replaced by subpoenas and court orders supported by "articulable facts" that are "relevant" to an investigation, the role of the judge in the process is diminished to nothing more than a decorative seal of approval. In many circumstances, neither court orders nor subpoenas are required.

Daniel Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1150–51 (2002).

C. The Current Remedies of Internet Surveillance Law

Statutory suppression remedies historically have been an important part of the enforcement mechanisms of electronic surveillance law. From the 1930s until 1968, no telephone wiretapping evidence was admissible in federal court.[59] Even today, the fruits of unlawful telephone wiretapping ordinarily must be suppressed as a matter of statutory law.[60] The statutory suppression remedy applies only to Wiretap Act violations: voicemails obtained in violation of the Stored Communications Act and non-content information obtained in violation of the Pen Register statute will not be suppressed as a matter of statutory law.[61]

In the Internet context, however, none of the laws contain a statutory suppression remedy, not even the Wiretap Act.[62] In 1986, when Congress passed ECPA, Congress agreed to accept Department of Justice's ("DOJ") proposal to reject a statutory suppression for Wiretap Act violations involving computer communications.[63] Little is publicly known about the reasons behind DOJ's request (and Congress's agreement) to exclude a statutory suppression remedy.[64] In all likelihood, DOJ worried that a suppression remedy would prove unduly harsh given the uncertain state of the law. Forcing the DOJ to comply with the complex new laws was one thing; suppressing evidence that the government collected in good faith under interpretations of the law that courts later rejected was another. Whatever the exact reason, DOJ's view prevailed and the law did not include a suppression remedy.

Instead, Congress enacted a powerful set of civil remedies to enforce the surveillance statutes. Under the Wiretap Act, any person

59. Wiretapping evidence was inadmissible in federal court under the Communications Act of 1924, Pub. L. No. 108-3 (1924) (current version at 47 U.S.C. § 605 (2003)), as first construed in *Nardone v. United States*, 302 U.S. 379, 382 (1937). The Supreme Court ruled that this exclusionary rule did not apply in state court in *Schwartz v. Texas*, 344 U.S. 199, 203 (1952). However, in 1968, just two days before Congress passed the modern Wiretap Act, the Supreme Court reversed itself and concluded that § 605 did bar wiretapping evidence in state court as well. *See* Lee v. Florida, 392 U.S. 378, 386 (1968).

60. *See* 18 U.S.C. §§ 2515, 2518(10)(a) (1993). However, the law as to when illegal wiretapping actually leads to suppression is quite complicated.

61. *See* 18 U.S.C. § 2708 (1993) (Stored Communications Act) ("The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter."); United States v. Fregoso, 60 F.3d 1314, 1320–21 (8th Cir.1995) (noting the absence of a statutory suppression remedy for the Pen Register statute).

62. *See* United States v. Meriwether, 917 F.2d 955, 960 (6th Cir. 1990); 18 U.S.C. § 2712(d) (Supp. 2002) (covering both the Stored Communications Act and Wiretap Act).

63. *See* Leib, *supra* note 11, at 409–11.

64. Michael Leib summarizes the horsetrading between Congress and the DOJ that led to the compromise. *Id.* at 109–11.

whose Internet communications are intercepted in violation of the Act can recover actual or statutory damages (whichever is greater), plus reasonable attorney's fees and other litigation costs,[65] plus punitive damages "in appropriate cases."[66] Persons aggrieved by violations of the Stored Communications Act can recover actual or statutory damages (whichever is greater), plus reasonable attorney's fees and other litigation costs,[67] and punitive damages in the case of willful or intentional violations.[68] Congress believed that these remedies were so important that it recently passed a second set of civil remedies as part of the USA PATRIOT Act, specifically allowing for suits against the federal government that contain unusually high statutory damages, plus reasonable litigation costs.[69] Oddly, Congress has failed to include an explicit civil remedy for violations of the Pen Register statute. Whether the Pen Register statute could support a private right of action is unclear; apparently no such suit has ever been brought. Despite this apparent oversight, taken as a whole the civil remedies offered by the Internet surveillance statutes provide strong incentives to sue. The combination of statutory damages, attorney's fees, and even punitive damages creates a considerable incentive for potential plaintiffs to raise their claims in court.

The surveillance laws do offer other remedies beyond civil remedies, but they are only rarely invoked. First, each of the statutes includes at least some criminal prohibitions. Willful violations of the

65. 18 U.S.C. § 2520(b)(3) (1993) ("In an action under this section, appropriate relief includes . . . a reasonable attorney's fee and other litigation costs reasonably incurred.").

66. *Id.* § 2520(b)(2) ("In an action under this section, appropriate relief includes damages under subsection (c) . . . .").

> If the person who engaged in that conduct has not previously been enjoined under § 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $50 and not more than $500.

Id. § 2520(c)(1)(A).

67. *Id.* § 2707(b)(3) (Supp. 2002) ("In a civil action under this section, appropriate relief includes . . . a reasonable attorney's fee and other litigation costs reasonably incurred.").

68. *Id.* § 2707(c).

> The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

Id.

69. *See id.* § 2712.

Wiretap Act are felony crimes,[70] albeit not ones that are likely to lead to prison time under the federal sentencing guidelines.[71] Violations of the Pen Register statute are mere misdemeanor crimes,[72] as are most of the few criminal violations of the Stored Communications Act.[73] Similarly, judicial or administrative findings that "serious questions" exist as to whether a federal government employee willfully violated the Wiretap Act or Stored Communications Act automatically trigger a proceeding into whether disciplinary action is warranted.[74] While these different approaches may help bolster the enforceability of the surveillance laws, they do not change the fact that the cases construing the laws will most likely deal with civil remedies.

II. The "Fog" of Internet Surveillance Law and Its Origins in the Current Remedies Scheme

This Section argues that the unusual statutory remedies scheme of Internet surveillance law has had profound consequences for the clarity and shape of Internet surveillance law. Thanks to the remedies scheme, courts rarely encounter disputes involving the Internet surveillance statutes, and when they do, the cases tend to be civil disputes that have little to do with the core concerns of criminal

70. *See id.* § 2511 (1993 & Supp. 2002) (making willful interception of an oral, wire or electronic communication a felony offense).

71. *See* U.S. SENTENCING GUIDELINES MANUAL § 2H3.1 (2000) (making a violation of 18 U.S.C. § 2511 a base 9 offense under the federal sentencing guidelines).

72. *See* 18 U.S.C. § 3121(d) (Supp. 2003). ("Whoever knowingly violates [18 U.S.C. § 3121(a)] shall be fined under this title or imprisoned for not more than one year, or both.").

73. *Id.* § 2701(b) states:

> The punishment for an offense under subsection (a) of this section is—
>
> (1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain—
>
> (A) a fine under this title or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and
>
> (B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and
>
> (2) a fine under this title or imprisonment for not more than six months, or both, in any other case.

74. *Id.* § 2712(c).

> If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted.

Id. See also id. § 2520(f) (Wiretap Act); *id.* § 2707(d) (Stored Communications Act).

investigations. The argument proceeds in three parts. First, the absence of a suppression remedy has resulted in few legal opinions, which has made the law unusually difficult to understand. Second, the absence of decisions interpreting the statutes in routine criminal cases has left many important questions unresolved. And third, the available civil remedies have produced an unusual number of influential opinions involving civil disputes far from the concerns that motivated Congress to pass the statutes, in which the courts simply get it wrong.

A. The "Fog" of Internet Surveillance Law

The law of electronic surveillance is famously complex, if not entirely impenetrable. Even before Congress added the Internet to the surveillance laws in 1986, the Fifth Circuit described the Wiretap Act as "a fog of inclusions and exclusions"[75] that frustrated the judicial search for "lightning bolts of comprehension."[76] The same court has since explained that that "construction of the Wiretap Act is fraught with trip wires,"[77] and in a case involving the intersection between the Wiretap Act and the Stored Communications Act, that the law is "famous (if not infamous) for its lack of clarity."[78] The Ninth Circuit has remarked that the Fifth Circuit's complaints "might have put the matter too mildly," and agreed that the surveillance laws involve "a complex, often convoluted, area of the law."[79] More recently, the Ninth Circuit reversed its own panel decision applying the Wiretap Act and the Stored Communications Act to the Internet,

75. *See* Briggs v. Am. Air Filter Co., 630 F.2d 414, 415 (5th Cir. 1980) (Goldberg, J.).

76. *Id.* The court's entire comment was the following:

> We might wish we had planted a powerful electronic bug in a Congressional antechamber to garner every clue concerning Title III, for we are once again faced with the troublesome task of an interstitial interpretation of an amorphous Congressional enactment. Even a clear bright beam of statutory language can be obscured by the mirror of Congressional intent. Here, we must divine the will of Congress when all recorded signs point to less than full reflection. But, alas, we lack any sophisticated sensor of Congressional whispers, and are remitted to our more primitive tools. With them, we can only hope to measure Congress' general clime. So we engage our wind vane and barometer and seek to measure the direction of the Congressional vapors and the pressures fomenting them. Our search for lightning bolts of comprehension traverses a fog of inclusions and exclusions which obscures both the parties' burdens and the ultimate goal.

Id. *See also* Fleming v. United States, 547 F.2d 872, 873 (5th Cir. 1977) ("Our analysis of the two statutory provisions makes us confident of only one conclusion: the statute is not a model of clarity.") (construing 18 U.S.C. §§ 2515, 2517 (1993 & Supp. 2002)).

77. Forsyth v. Barr, 19 F.3d 1527, 1542–43 (5th Cir. 1994).

78. Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994).

79. United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998).

explaining in its latter opinion that Internet surveillance remained "a confusing and uncertain area of the law."[80]

The complexity of the surveillance laws owes in part to their history. The statutory language and structure reflect the technology of the eras in which Congress enacted the different pieces of the statutory puzzle. The 1968 Wiretap Act reflects the technology and practices of the 1950s and 1960s telephone networks; the 1986 Stored Communications Act uses early 1980s terminology about the Internet and computer networks. This disparity in approaches does not necessarily mean that the law is outdated. Once understood, the laws reveal a surprisingly workable, if not masterful, framework. Many hours of study unearth a surprising amount of thought and wisdom in the statutory text.

But before attaining mastery of the materials, a student must slowly work her way through remarkably difficult statutory language. What on earth is a "pen register,"[81] a student might wonder, or a "trap and trace device"[82]? What's the difference between a "remote

80. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002). The Ninth Circuit blamed this confusion on Congress's failure to update the law to take into account modern technologies. In particular, the court complained that:

> the difficulty [in construing the surveillance statutes] is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication .... Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results.

Id. While the court is correct that the law remains complex, the court is wrong that the reason for the complexity lies in Congress' failure to account for the Internet. ECPA was enacted in order to protect the privacy of Internet communications. The idea that ECPA was written *before* the Internet was invented is quite preposterous (although, in fairness, the court's claim that ECPA was written before the *World Wide Web* is correct).

81. "Pen register" is defined as:

> a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

18 U.S.C. § 3127(3) (Supp. 2002).

82. "Trap and trace device" is defined as:

> a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

Id. § 3127(4).

computing service,"[83] and an "electronic communication service"[84]? What is the difference between a "wire communication"[85] and an "electronic communication"[86]? Why does the Wiretap Act only prohibit interception of communications using a "device,"[87] but then exempt from the definition of devices any equipment provided by a provider to a user and used by the user "in the ordinary course of its business"[88]? Why does the statutory definition of "electronic storage" exclude most communications that are stored electronically?[89]

---

83. "Remote computing service" is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system...." *Id.* § 2711(2).

84. "Electronic communication system" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* § 2510(15) (1993).

85. "Wire communication" is defined as:

> any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.

Id. § 2510(1) (Supp. 2002).

86. "Electronic communication" is defined as:

> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—(A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

Id. § 2510(12)

87. *Id.* § 2511 (1993 & Supp. 2003) prohibits interceptions, and *id.* § 2510(4) defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device...."

88."[E]lectronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than—

> (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties.

Id. § 2510(5)(a).

89. *See* 18 U.S.C. § 2510(17); Konop v. Hawaiian Airlines, 302 F.3d 868 (9th Cir. 2002).

While all of these questions have answers if you know where to look,[90] few if any of those answers can be found in published judicial decisions. Judicial decisions often guide the way through complex areas of law: a well reasoned and clear opinion can explain in basic language what a complex statute does and how it works. Yet despite the fact that ECPA was passed over fifteen years ago, very few judicial opinions have interpreted the laws that ECPA created. A student wishing to learn the law by seeing how courts apply it in actual cases will quickly become frustrated. The Internet has become a routine part of life for over a hundred million Americans,[91] but those who wish to learn the laws that govern Internet surveillance have few options but to work their way through the raw statutory text, term-of-art by term-of-art.[92] Few cases explain what the complicated words mean in relatively clear language that a lawyer or law student can readily understand.

A few Westlaw queries reveal the scope of the problem. The ALLFEDS database contains only forty-six judicial decisions after 1985 that cite any of the electronic surveillance statutes in the same paragraph that the word "computer" appears.[93] Think about that: forty-six cases in sixteen years. Thirty-four of these cases cite the Wiretap Act, and twenty-two of them cite the Stored Communications Act while ten cases cite both.[94] None of the cases cite the Pen Register statute. Admittedly, my methodology is highly unscientific. I do not doubt that several relevant cases have fallen beyond this query, and that the result of the query includes many

90. Some answers derive from contemporary understandings of communications technology at the time the text became law. Other answers can be explained by distinctions drawn by long-forgotten judicial opinions. I explain the difference between "pen registers" and "trap and trace devices" (as well as the historical reason for their unusual names) and historical development in Kerr, *supra* note 30, at 632–33. The difference between remote computing service and electronic communications service, and between wire communications and electronic communications, is explained in the CCIPS Manual, *supra* note 3, ch. 4. The exception in definition of "device", sometimes known as the extension telephone exception to the Wiretap Act, traces back to a 1957 Supreme Court decision interpreting the 1934 Communications Act. Rathbun v. United States, 355 U.S. 107 (1957). In *Rathbun*, Chief Justice Warren held that the Communications Act allowed the use of "extension telephones." *Id.* at 110. Congress carved out an exception to the definition of "device" to create consistency between the Wiretap Act and the Communications Act it replaced.

91. Pew Research Center, Internet Activities *at* http://www.pewinternet.org/reports/chart.asp?img=Internet_Activities.jpg (last visited March 25, 2003).

92. Although I am hardly unbiased in making such a recommendation, I believe that a notable exception is the CCIPS Manual, *supra* note 3.

93. I ran the following search on October 5, 2002 in the Westlaw ALLFEDS database: "18 U.S.C." /2 (2510 2511 2512 2513 2514 2515 2516 2518 2520 2701 2702 2703 2704 2705 2706 2707 2708 2711 3121 3122 3123 3124 3125 3127) /p computer & DA(AFT 1985).

94. This result was based on the results from the search in the footnote above.

cases that merely cite the statutes but do not actually apply them.[95] But the general point survives. In the more than fifteen years since Congress enacted the modern Internet surveillance laws, only a trickle of cases have emerged that shed light on any part of them.

Why? The blame lies squarely with the remedies scheme that Congress has chosen to enforce the surveillance laws. Because Congress has not provided a statutory suppression remedy, criminal defendants have little incentive to raise challenges to the government's Internet surveillance practices. Absent defense challenges, courts rarely encounter disputes alleging violations of those laws, and few decisions result. We can see the difference by comparing the number of cases after 1985 that cite the Wiretap Act in the same paragraph that the word "computer" appears with cases that cite the Act in the same paragraph as the word "telephone" (recall that the Wiretap Act contains a suppression remedy in the telephone context). In the former, only thirty-two cases in Westlaw's ALLFEDS database qualify; in the latter, 908 cases do.[96] While this may reflect the greater number of telephone wiretaps than Internet wiretaps, at least in part, a comparison of the number of cases that cite the Wiretap Act (which offers a suppression remedy in some contexts) and the Pen Register statute (which does not) reveals a similar trend. Altogether, 1,498 cases in the ALLFEDS database have cited the Wiretap Act since January 1, 1986;[97] in the same time, only forty cases have cited the Pen Register statute.[98] In other words, cases citing the Wiretap Act outnumber those citing the Pen Register statute by a ratio of about forty to one. This disparity exists despite the fact that in most criminal investigations, the number of pen register orders the government obtains usually outnumbers the number of wiretap orders by a factor of about ten to one.

Thanks to the lack of a statutory suppression remedy, few defendants bother to challenge the government's Internet surveillance practices. When defendants raise these challenges, the courts generally reject them without reaching the merits on the ground that no suppression remedy exists. Exceptions do exist. On

95. And of course, a citation that appears in the same paragraph as the word "computer" does not mean that the case concerns the substance of the statutes. Although this categorization is necessarily subjective, I would estimate that only about half of those opinions, roughly twenty in all, offer any interpretation (however brief) of how the surveillance statutes apply to computers and the Internet.

96. I ran the following query in the ALLFEDS database on October 5, 2002: "18 U.S.C." /2 (2510 2511 2512 2513 2514 2515 2516 2518 2520) /p computer & DA(AFT 1985), and then the same with "telephone" replacing "computer."

97. I ran the following query in the ALLFEDS database on October 5, 2002: "18 U.S.C." /2 (2510 2511 2512 2513 2514 2515 2516 2518 2520) & DA(AFT 1985).

98. I found this by running the same search as above, but with the sections of Title 18 that make up the Pen Register statute substituted for the Wiretap Act sections.

rare occasions, a court will nonetheless touch on the merits of defendant's claims. For example, in *United States v. Kennedy*,[99] a defendant challenged the government's failure to comply with the statutory requirement of including "specific and articulable facts" in an application for a court order to compel an ISP to divulge information pursuant to section 2703(d) of the Stored Communications Act. The information had allowed the government to connect the defendant to reports of child pornography, which led to a search warrant executed at the defendant's home, which led to the discovery of child pornography on the defendant's home computer. The court agreed with the defendant, concluding that the government's application did not supply a sufficient factual basis; but then ruled against the defendant on the ground that suppression was unavailable as a remedy.[100] Finding no constitutional defect in the warrant itself, the court ruled against the defendant and allowed the evidence to be used against him.[101]

Although the *Kennedy* court rejected the defendant's suppression argument, the case is unusual because the defendant was willing to raise a statutory surveillance argument, and the court was willing to evaluate it on the merits.[102] In most criminal cases, defendants will not raise such arguments, and the question of whether the government's investigation complied with Congress's rules will remain unanswered.

B. Legal Questions That Remain Unanswered

I have focused so far on how the absence of a suppression remedy in the Internet surveillance statutes has led to few legal decisions interpreting the statutes, which in turn has made it difficult for courts, lawyers, and law students to make sense of the laws without wading through difficult statutory text. My concern has been

99. 81 F. Supp. 2d 1103 (D. Kan. 2000).

100. Ironically, the government in the *Kennedy* case did not need to get a 2703(d) order at all—the government was merely requesting to know the identity of the relevant subscriber, which it could have obtained with a subpoena pursuant to 18 U.S.C. 2703(c)(1)(C) (1996).

101. *See id.*

102. Another rare case in which this occurred (or at least something similar to it) is *United States v. Scarfo*, 180 F. Supp. 2d 572 (D.N.J. 2001). In *Scarfo*, the defendant tried to argue that the government's failure to comply with the Wiretap Act in the course of installing a monitoring device in his home computer should have led to suppression of the evidence obtained through the monitoring. *Id.* Making much ado of a fairly simple legal problem, the Court held on the merits that the Government's monitoring device had not violated the Wiretap Act. *Id.* at 582. For a 1940s era version of the *Scarfo* case, see Goldman v. United States, 316 U.S. 129, 134 (1942) (rejecting a similar argument under the predecessor to the Wiretap Act following the installation of a monitoring device called a "detectaphone").

with the difficulty of finding the existing answers and understanding the decisions Congress clearly made. This same dynamic has produced a related effect, however. By shielding routine investigative steps from judicial review in the context of suppression hearings, Congress has made it difficult for the courts to resolve major disputes over the interpretation of the Internet surveillance statutes. Whereas the courts would normally provide a forum to interpret and clarify Congress's handiwork, the current remedies scheme has largely limited the judicial role to reviewing applications for court orders during investigations, rather than evaluating the laws in written opinions after criminal charges have been filed.

(1) The Scope of the Pen Register Statute Before the USA PATRIOT Act

The uncertainty over the scope of the Pen Register statute before the passage of the USA PATRIOT Act in October 2001 provides a helpful illustration of the problem. Before the PATRIOT Act, the text of the Pen Register statute did not clearly state whether it also applied to computer communications and the Internet.[103] The stakes were significant. If the Pen Register statute did not apply to computers and the Internet, then anyone could wiretap the Internet without any court order or judicial review whatsoever, so long as the wiretap filtered out the "contents" of communications.[104] At the same time, the government would need a search warrant based on probable cause to compel an ISP to conduct such monitoring on its behalf. If the Pen Register statute did apply to the Internet, however, then such surveillance was a federal crime, but the government could obtain a pen register order under a very low threshold (much lower than a search warrant standard) that could compel the ISP to conduct monitoring for the government.[105]

So did the Pen Register statute apply to the Internet? The Justice Department believed it did, and its lawyers regularly applied for pen register orders to conduct Internet surveillance, which magistrate judges regularly signed.[106] But because no suppression remedy existed for violations of the Pen Register statute, no criminal defendants ever challenged this practice, and no Article III judge ever had the opportunity to decide whether the statute applied to the Internet. Obtaining pen register orders became an important and established part of the government's Internet surveillance practices, but the only judges to evaluate the practices were the magistrate judges who either agreed with the government and signed the orders

103. *See* Kerr, *supra* note 30, at 632–36.
104. *See id.* at 634.
105. *See id.*
106. *See id.*

or disagreed with the government and refused.[107] No published decisions existed to help explain the scope of the statute. Until Congress clarified that the statute did apply to the Internet as part of the USA PATRIOT Act, the question remained uncertain.

(2) The Wiretap Act and the "Party to the Communication" Exception

Current uncertainty over how the Wiretap Act's "party to the communication" exception applies to computer networks provides another helpful example.[108] The Wiretap Act was designed to apply to the telephone network, and prohibits the use of a device to intercept a communication sent between two parties.[109] If Bob speaks on the phone to Mary, third-party Joe cannot tap the line using a wiretapping device and listen in. However, the Wiretap Act contains an exception that allows any "party to the communication" to wiretap the line, or to consent to others doing so.[110] The key question is, who is a party to the communication? The answer is critical because a party can wiretap the communication and a non-party ordinarily cannot. In the telephone context, the availability of a suppression remedy has led to many cases that together draw a relatively clear rule that a party to the communication is the human being on the end of the line.[111] In the case of the phone call between Bob and Mary, both Bob and Mary are parties to the communication; Joe is not.

How the party to the communication exception applies to the Internet has tremendous importance for Internet surveillance law. As explained earlier, the Internet works on a principle of communal sharing of information: a computer user might send a command to computer A, asking computer A to route a command though computer B and deliver it to computer C. The question is, who (other than the user) is a party to the communication? Is A a party to the communication between it and the user? Is C a party? How about B? These questions are vitally important, but no one really knows the answers. The courts have not had the opportunity to answer these

107. Two unpublished magistrate decisions were decided in 2000 that evaluated the question. *See* Kerr, *supra* note 30, at 634–35. In one case in the Central District of California, an ISP challenged the government's order, and the magistrate judge agreed with the government that the statute applied to the Internet. In another case in the Northern District of California, a magistrate judge received an application and disagreed with the government, writing an opinion in the *ex parte* matter explaining that she did not believe the statute applied to the Internet. *Id.* at 635.

108. *See* 18 U.S.C. § 2511(2)(c), (d) (1993 & Supp. 2002).

109. *See id.* § 2511.

110. *See id.* § 2511(2)(c), (d) (Supp. 2002).

111. *See, e.g.*, United States v. Eschweiler, 745 F.2d 435, 437 (7th Cir. 1984) (holding that government informant on the line was a party to the communication); United States v. Gallo, 659 F.2d 110, 114 (9th Cir. 1981) (police officer answering the phone during the execution of a warrant was a party to the communication).

questions in any depth. In the very early case of *United States v. Seidlitz*,[112] a computer hacker argued that the owners of the computer he hacked had violated the Wiretap Act when they recorded the hacker's unauthorized commands sent to the hacked computer. The Fourth Circuit rejected the claim first on the ground that the Wiretap Act did not apply to computers (which was true at that time, several years before ECPA).[113] Then, in dicta, the Court added that the hacker's claim could also fail because the victim computer was "for all intents and purposes a party to the communication."[114] Similarly, in *United States v. Mullins*,[115] a user of an American Airlines computer network argued that the airline violated the Wiretap Act by recording the unauthorized travel arrangements he had made using the network. The Court quickly rejected the argument on several grounds, among them the unexplained conclusion that "one of the parties to the communication (viz., American [Airlines] . . .) had consented to the monitoring."[116]

That's it, however.[117] Together, *Seidlitz* and *Mullins* suggest that the victim of a hacker's commands is probably a party that can record the hacker's attack, but whether this is true and to what extent actually remains quite unclear. Because a criminal defendant cannot move for suppression of the evidence on the basis of a Wiretap Act violation, the courts have faced few opportunities to apply the telephone's legal framework to the Internet in criminal cases. As a result, a very basic question that underlies how the Wiretap Act applies to the Internet remains largely unknown. Congress can always step in and clarify the law, as Congress did in part when it passed the USA PATRIOT Act, but under the current remedies scheme courts have had few opportunities to develop and clarify the law.[118]

112. 589 F.2d 152, 157–58 (4th Cir. 1978).

113. *Id.* at 157.

114. *Id.* at 158.

115. 992 F.2d 1472, 1478 (9th Cir. 1993).

116. *Id.*

117. One possible exception is *In re* DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001), discussed at length below.

118. One interesting implication of this dynamic is that there are some parts of ECPA that exist on the books but have little or no effect whatsoever, and seem unlikely to ever receive any judicial attention (or legislative repeal). The most obvious example of this is 18 U.S.C. § 2704 (2002), which is entitled Backup Preservation. Section 2704 is part of the original 1986 Act, and offers a complex procedure in which the government can order an ISP to make a backup of a communication to preserve the communications. The section was made largely redundant by the later addition of 18 U.S.C. § 2703(f) (2002), which requires ISPs to take "all necessary steps" to preserve evidence when contacted by law enforcement and informed that a court order for the evidence is being sought. As a result of advances in both the law and technology, section 2704 no longer serves any purpose, and is never used.

C. The Distorting Effects of Civil Precedents

The law's current focus on civil remedies has produced a third unfortunate effect on the development of Internet surveillance law: the emergence of civil precedents that misconstrue the surveillance laws almost beyond recognition, and end up making the law more confusing, not less.

(1) How Civil Cases Can Distort Criminal Statutes

It is not hard to see why the current remedies scheme encourages the filing of civil lawsuits that stretch the boundaries of the electronic surveillance statutes. The promise of attorney's fees and the possibility of punitive damages, combined with the added bonus of a federal question to allow the suit to be filed in federal court, creates a strong incentive for potential plaintiffs to push the boundaries of Title III and ECPA in civil cases. As a result, about seventy percent of the cases in the Westlaw ALLFEDS database that cite the surveillance statutes in cases involving computers are civil cases. Most of these suits do not involve the government at all: rather, they involve claims that a private party invaded the plaintiff's Internet privacy, and that the invasion of privacy should be considered a "wiretap" or a violation of the Stored Communications Act.

In the abstract, whether a case appears on the criminal or civil side of a court's docket may seem irrelevant to how the court resolves the legal issue. The law is the law, and the statutory text is the statutory text. However, the dramatically different context of the two types of cases inevitably pulls at how courts interpret the laws. Consider the forces at play when a criminal defendant challenges the government's surveillance practices in a motion to suppress. Courts naturally will interpret the statutes in light of the necessary balance between a defendant's civil liberties on one hand and the government's need to solve crimes on the other. If a court construes the statutes too narrowly, it may infringe upon the defendant's civil liberties (and by implication, our own); if the court construes the surveillance statutes too broadly, it may unduly restrict law enforcement's ability to protect public safety.

The stakes are quite different in a typical civil case between private parties. In a civil case, plaintiff A will come forward alleging a violation of his Internet privacy by the defendant B. The case may have nothing whatsoever do to with criminal law. Instead, party A will claim that party B did something that infringed on party A's privacy interests, and that party B should have to pay, at least in part. Courts naturally will interpret the applicable law in light of the normative question of which party should bear the costs of the harm and in what proportion. If the court construes the statute too

narrowly, it may force A to bear the costs of B's harmful conduct. If the court construes the statute too broadly, it may force B to bear costs better borne by A. Either way, when the court tries to strike that balance, the court will view the case through the lens of tort law rather than criminal law.

These differences assume tremendous importance when a court must resolve a civil dispute based on the predominantly criminal Internet surveillance laws. Owing to the near-total absence of criminal precedents interpreting these statutes, a court often will have little sense of how its decision fits within the context of criminal cases, or even that the decision will have any implications at all for criminal law. The court will try to wade through the inscrutable statutory text of ECPA and Title III guided by an intuitive need to distribute costs properly between the private parties, with little sense of how its decision will affect the world of criminal law and law enforcement surveillance practices. When the resulting civil precedents are applied in a criminal context, however, the decisions can have surprising and disturbing implications for routine criminal investigations.

(2) In re Doubleclick Privacy Litigation

Consider the recent civil litigation over Doubleclick, an Internet advertising service.[119] Doubleclick's service worked by placing a "cookie" on Internet user's computers that contained information about other websites that the computer had been used to visit within a network of companies that used Doubleclick's service. When a user browsed the web and visit different sites that were Doubleclick customers, Doubleclick's server sent the computer targeted advertising based on the other sites that the user had visited.[120] A casual user would not know that his computer was communicating with Doubleclick's server as the process was mostly invisible to the user. In theory, this approach allowed Doubleclick to target advertising, allowing companies wishing to advertise to reach interested customers more easily (and allowing Doubleclick to make a buck in the process).

But plaintiffs' lawyers weren't far behind. Seeking attorney's fees and punitive damages, plaintiffs' lawyers pounced on the case, suing Doubleclick in various federal districts for violating the Wiretap Act and the Stored Communications Act, among other laws. The cases were consolidated as a single massive class action in the Southern District of New York, and brought on behalf of all Internet

119. *See In re DoubleClick*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001).
120. *See id.* at 500–05.

users who had Doubleclick cookies placed on their computers.[121] The plaintiffs' theory was that by placing cookies on the plaintiffs computer and sending communications to and from the computers behind the scenes, Doubleclick had both accessed the computers of communications providers without authorization, thereby obtaining communications in electronic storage in violation of the Stored Communications Act, and wiretapping the users' computers in violation of the Wiretap Act.[122]

Both of these claims were quite ridiculous. Recall that the Stored Communications Act regulates the privacy of Internet account holders at ISPs and other servers; the law was enacted to create by statute a set of Fourth Amendment-like set of rights in stored records held by ISPs.[123] The theory of the Doubleclick plaintiffs turned this framework on its head, as it attempted to apply a law designed to give account holders privacy rights in information held at third–party ISPs to home PCs interacting with websites. In the language of the client/server network model, the plaintiffs tried to harness a law designed to give clients rights in communications held by their server by recasting the clients as servers and the websites they visited as the clients. The plaintiffs then wanted the Act to give servers privacy rights against invasions of privacy by their clients, rather than vice versa.

The plaintiffs' Wiretap Act claims were only slightly less absurd. As explained earlier, the Wiretap Act prohibits a third-party from intercepting in real-time the contents of communications between two parties unless one of the two parties consents. This law had no applicability to Doubleclick's cookies, as the cookies did not intercept any contents and did not intercept anything in real-time. The cookies merely registered data sent to it from Doubleclick's servers. As the plaintiffs construed the Wiretap Act, however, the cookies were "wiretaps" that intercepted their users communications just like a telephone wiretap.

Faced with the plaintiffs' civil complaint and Doubleclick's motion to dismiss, however, the District Court accepted the basic framework offered by the plaintiffs (although it did find exceptions in the laws that allowed it to rule in favor of the defendants).[124] Most importantly, the court agreed with the plaintiffs' patently absurd argument that home PC users were "providers" regulated by the Stored Communications Act, and that the Act gave "providers"

121. *See id.* at 500.
122. *See id.* at 501.
123. *See* S. REP. NO. 99-541, (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.
124. *See In re DoubleClick*, 154 F. Supp. 2d at 509–14 .

privacy rights against "users," in this case websites.[125] This is something like going into court and deciding that the judge is the plaintiff, the jurors are the defendant, and that the question is whether the bailiff has to pay damages to the court clerk. It's hard to imagine a court reaching such a result in a criminal case. The Act allows the government to obtain court orders compelling providers to disclose records about their users,[126] and no prosecutor would obtain a court order compelling a home personal computer to disclose records about a website. Similarly, in the case of the Wiretap Act claims, the defendant *conceded* the incorrect assertion that the cookie was a wiretap for the purposes of its motion,[127] and argued only that the cookie did not violate the wiretap act because Doubleclick's server was a "user" and therefore a "party to the communication," which the Court agreed it was.[128] Again, it's difficult to imagine a criminal court applying such a framework in a criminal case: any prosecutor who works with wiretaps would know that a cookie simply does not effectuate a wiretap.

Unable to find any criminal precedents directly on point, however, and unaware of how its decision would apply in a criminal context, the district court agreed with the bizarre framework offered by the civil lawyers in the case. The result was an opinion on the books that misinterprets the Internet surveillance laws pretty much from start to finish, with hardly a single correct assertion of law.[129] And yet given the near total absence of cases interpreting the statutes, the *Doubleclick* opinion stands as one of the few published precedents on how the surveillance laws apply to the Internet. In fact, in the year and a half since the case appeared, no less than *five* law school casebooks on Internet law and privacy law have already featured the *Doubleclick* case as a leading case to explain Internet

125. *See id.* at 510.

126. *See, e.g.*, 18 U.S.C. § 2703(d) (Supp. 2002).

127. *See In re Doubleclick*, 154 F. Supp. 2d at 514 ("For the purposes of this motion, DoubleClick concedes that its conduct, as pled, violates this prohibition [in the Wiretap Act]. However, DoubleClick claims that its actions fall under an explicit statutory exception . . . .").

128. *See id.*

129. Ironically, the Court did make one correct conclusion of law, although under a quite bizarre rationale. The Court properly concluded that the prohibition in 18 U.S.C. § 2701 applies only to the access of communications in "electronic storage," which is defined to mean temporary intermediate storage pending delivery, such as an e-mail that has not yet been delivered. *Id.* at 512. To reach this result, however, the court relied heavily on a House Report and text relating to a *bill from the year 2000* that was proposed *but never passed* that contained language purporting to explain the meaning of "electronic storage." *See id.* (*quoting* H.R REP. NO. 106-932 (2000)). Reliance on legislative history is one thing, but reliance on the legislative history of a bill that was proposed but never passed fifteen years after the passage of the legislation at issue was enacted seems quite another. On this one question, however, it so happened that the court's result was correct.

surveillance law.[130] The hallucinogenic interpretations of the statutes in *Doubleclick* have been treated as important precedents among lawyers and law students eager to understand the mysteries of the Internet surveillance laws.

(3) Konop v. Hawaiian Airlines

The Ninth Circuit's initial decision in *Konop v. Hawaiian Airlines*[131] *(Konop I)* offers a second example of how courts can dramatically misconstrue the Internet surveillance laws in civil cases. Robert Konop was a Hawaiian Airlines pilot who maintained a password-protected website which contained his workplace grievances.[132] Konop provided usernames to specific airline employees, who could then log on to the site, obtain a password, and then access the password-protected portions of the site to view Konop's opinions on the airline and its union.[133] Davis, a vice-president of the airline, caught wind of the site and obtained permission from an employee who was assigned a username (but had not himself obtained a password) to log on to the site with the employee's username to view Konop's materials.[134] When Konop learned that Davis had viewed the website, Konop sued the airline in federal court, alleging—you guessed it—violations of the Wiretap Act and the Stored Communications Act.[135]

Both of Konop's claims should have been swiftly rejected. The Wiretap Act arguments lacked merit because the Act addresses only prospective, real-time surveillance, the statutory embodiment of the Fourth Amendment principles developed by the Supreme Court in the real-time wiretapping case of *Berger v. New York*.[136] Under the trio of surveillance laws, access to stored communications such as web files is governed if it all by the Stored Communications Act, not the Wiretap Act.[137] Konop's Stored Communications Act claim should have failed as well. Konop sued under a provision that only prohibits

130. *See* RAYMOND KU ET AL., CYBERSPACE LAW; CASES AND MATERIALS 559–67 (2002); RONALD J. MANN & JANE K. WINN, ELECTRONIC COMMERCE 140–48 (2002); DANIEL SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW, 493-503 (2002); MADELEINE SCHACTER, THE LAW OF INTERNET SPEECH 434–45 (2002); MADELEINE SCHACTER, INFORMATIONAL AND DECISIONAL PRIVACY (2002).

131. 236 F.3d 1035 (9th Cir. 2001), *withdrawn*, 262 F.3d 972 (9th Cir. 2001), *modified*, 302 F.3d 868 (9th Cir. 2002).

132. *See Konop*, 236 F.3d at 1042.

133. *See id.*

134. *See id.*

135. Konop also alleged violations of the Railway Labor Act, 45 U.S.C. §§ 151–88 (2002), but those arguments are not relevant here. *Id.* at 1048.

136. 388 U.S. 41 (1967).

137. *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994).

unauthorized access to files stored incident to transmission in a user's account held by a service provider,[138] such as undelivered, unopened e-mail held by an ISP. Web files held by a web server waiting to be sent to whoever accesses a web page cannot satisfy this threshold showing: in the language of the act, web page files are not files in temporary "electronic storage"[139] held by "a facility through which an electronic communication service is provided."[140]

But the Ninth Circuit would have none of this. Showing the judicial independence that has made the Ninth Circuit famous (or infamous, depending on your point of view), the court managed to fashion a remedy for the sympathetic plaintiff-employee against his overly intrusive defendant-employer on *both* the Wiretap Act and the Stored Communications Act claims. Rejecting the teachings of a dozen or so courts (including the Ninth Circuit itself[141]) in favor of two student law review notes and hints of broad commitments to protecting privacy found in the legislative history, the Court held that the Wiretap Act *did* apply to stored Internet communications.[142] The Court was influenced in large part by the fact that it could find no statute that governed access to stored communications: Congress must have intended that the Wiretap Act would protect stored communications, the court reasoned, because it did not protect them elsewhere.[143] Because it seemed arbitrary and irrational to protect communications in transit but not stored communications, the Court concluded that the Wiretap Act applied to access to stored

138. 18 U.S.C. § 2701(a) (Supp. 2002).

139. *Id.* The term "electronic storage" is defined in 18 U.S.C. § 2510(17) as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

140. 18 U.S.C. § 2701(a)(1).

141. United States v. Smith, 155 F.3d 1051, 1057–59 (9th Cir. 1998).

142. *See id.* at 1046 (citing Tatsuya Akamine, *Proposal for a Fair Statutory Interpretation: E-Mail Stored in a Service Provider Computer Is Subject to an Interception Under the Federal Wiretap Act*, 7 J.L. & POL'Y 519, 550–51 (1999); Thomas Greenberg, *E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U. L. REV. 219, 248–49 (1994)).

143. *See Konop*, 236 F.3d at 1045:

> [W]here Congress has provided lesser protection for electronic communications, it has done so straightforwardly, and for discernable reasons.... No similarly straightforward provision of the Wiretap Act affords stored electronic communications a lesser degree of protection from interception than stored wire communications. We know of no reason why Congress might have wished to do so. An electronic communication in storage is no more or less private than an electronic communication in transmission.

Id. As the Court later recognized, this statement overlooked the Stored Communications Act entirely.

communications and that Davis had violated the Wiretap Act by viewing Konop's website. The Court reversed the trial court's ruling to the contrary, noting in passing that its reversal on the Wiretap Act claim also required reversal on the Stored Communications Act claim, which the court viewed as merely a "lesser included offense" of the Wiretap Act claims.[144]

Whatever the merits of *Konop I* from the standpoint of employer-employee relations, the decision would have had potentially disastrous implications for Internet crime investigations had it stayed on the books.[145] The trouble is that the Stored Communications Act already governed access to stored communications, as its title suggests. Subjecting every kind of access to the "super search warrant" requirement of the Wiretap Act would have nullified the Stored Communication Act entirely, and brought many if not most Internet crime investigations to a standstill because nearly every step of an investigation would require the government to obtain a "super search warrant" wiretap order.[146] Understood as a whole, the Internet surveillance laws clearly did not contemplate this.

At the time of *Konop I*, however, the Ninth Circuit simply did not understand how Konop's claim fit within the broader context of the law. It construed the case through the lens of worker privacy, not the rules that govern criminal investigations. It was only when the implications of *Konop I* for criminal law reached the panel through *amicus* briefs filed by federal and state law enforcement interests in favor of the Airlines' petition for rehearing that the panel realized its error.[147] The panel eventually withdrew its initial decision, and a year

144. *See id.* at 1048. The *Konop* Court's strange notion that the Stored Communications Act provided a "lesser included offense" of the Wiretap Act derived from a misreading of the Stored Communications Act in *obiter dictum* by a prior Ninth Circuit panel in *Smith*. 155 F.3d at 1051. In that case, under the guise of a textualist reading of the intersection of the Stored Communications Act and the Wiretap Act, Judge O'Scannlain invented from whole cloth a novel theory that the former was a "lesser included offense" of the latter, and that the Stored Communications Act really had nothing to do with stored communications at all. *Id.* at 1058. Congress corrected this error, rejected *Smith*, and clarified the line between the Wiretap Act and Stored Communications Act when it passed the USA PATRIOT Act in October, 2001. As the *Konop II* panel recognized, the PATRIOT Act rejected the statutory basis for this "lesser included offense" theory. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d at 878 ("By eliminating storage from the definition of wire communication, Congress essentially reinstated the pre-ECPA definition of intercept—acquisition contemporaneous with transmission-with respect to wire communications.") (citations omitted).

145. *See* Caitlin Liu, *Reversal of Internet Ruling Is Sought: U.S. and Local Prosecutors Tell Appeals Court That Curbs on Web Site and E-Mail Access Make Their Job Harder*, L.A. TIMES, April 23, 2001, at B1.

146. *Id.*

147. I co-authored one of the amicus briefs on behalf of the Justice Department along with Mark Eckenwiler of the DOJ Computer Crime and Intellectual Property Section.

later issued a second decision (*Konop II*) that agreed that the Wiretap Act did not apply to stored communications.[148] Even in *Konop II*, however, the Court adhered to its view (implied in *Konop I*) that the Airlines vice-president had violated the Stored Communications Act.[149] Just like the defendants in the *Doubleclick* case wrongly conceded that the Wiretap Act applied, the defendant in *Konop* had wrongly conceded that the Stored Communications Act applied,[150] and based its argument solely on the application of an exception that the *Konop II* court ultimately rejected.[151]

In both *Konop I* and *Doubleclick*, courts faced civil disputes litigated by civil lawyers involving criminal statutes for which few criminal precedents existed. The courts did their best in light of what they knew. But faced with the fog of Internet surveillance law and the complex maze of statutes involved, both courts dramatically misconstrued the applicable law. Without any sense of how their decisions would apply in a criminal context, both courts erred in major ways that they could not envision. The statutes lacked a suppression remedy which would have filled the books with criminal cases settling key issues in a criminal context. As a result, courts forced to venture into this area in a civil context had little guidance to follow and produced results that confused rather than clarified the law.

III. Lifting the Fog of Internet Surveillance: A Proposal to Add a Statutory Suppression Remedy to the Internet Surveillance Laws

Internet surveillance law remains a fog, and the remedies scheme deserves much of the blame. What can Congress do to change this? In this section, I offer a proposal for Congress to enact a statutory suppression remedy for violations of the Internet surveillance statutes. To be more accurate, I offer a *range* of proposals. There are several ways in which Congress could enact a suppression remedy, and although I have a few preferences, I am ambivalent as to which approach would be best. After introducing the proposal, I offer

148. *See Konop*, 302 F.3d at 878.

149. *See id.* at 880.

150. *See id.* at 879–80.

> The parties agree that the relevant "electronic communications service" is Konop's website, and that the website was in "electronic storage." In addition, for the purposes of this opinion, we accept the parties' assumption that Davis' conduct constituted "access without authorization to a facility through which an electronic communication service is provided."

Id.

151. *See id.*

arguments in its favor addressed to two important constituencies that exert a significant influence over Congress in this area: civil liberties groups, such as the Center for Democracy and Technology[152] and the Electronic Privacy Information Center,[153] on one hand, and the Justice Department on the other. While it may seem unorthodox to frame arguments with these two groups explicitly in mind, few changes in the Internet surveillance statutes can pass through Congress without at least the support of one of these sides and the grudging acquiescence of the other.

A. A Proposal to Add a Suppression Remedy to the Internet Surveillance Laws

The core of my proposal is to make violations of the Internet surveillance statutes grounds for suppression of evidence in criminal cases. As I detail further below, such a change would create a strong incentive for defendants to challenge the government's surveillance practices in court. In so doing, it would create a forum for the courts to apply the statutes in criminal cases, which would clarify both to the government and the public what powers the government can exercise to investigate Internet crime, as well as the limits on those powers.

Two difficult and interrelated questions confront any effort to add a suppression remedy to the Internet surveillance statutes. The first question is, how broadly should the remedy extend? Congress could add a suppression remedy limited to violations of the Wiretap Act only, mirroring the current law of telephone surveillance. Congress could opt for a slightly broader approach, and limit the suppression remedy to statutory violations that involve the acquisition of contents (covering violations of the Wiretap Act and Section 2703 of the Stored Communications Act). On another axis, Congress could model the suppression remedy after the Fourth Amendment, and limit it to violations of the law by the government, rather than allowing the rule to encompass the suppression of evidence obtained by private parties in violation of the surveillance laws.[154] Finally, Congress could embrace a broad rule that extends the

152. http://www.cdt.org (last visited Oct. 5, 2002).

153. http://www.epic.org (last visited Oct. 5, 2002).

154. The Wiretap Act's suppression remedy applies to communications wrongfully intercepted by both the government and private parties. *See* 18 U.S.C. § 2518(10)(a)(i) (1993) (stating that an aggrieved person may move to suppress the contents of wire and oral communications when "the communication was unlawfully intercepted."); United States v. Vest, 813 F.2d 477, 481 (1st Cir. 1987).

The Sixth Circuit has carved out a "clean hands" exception to this rule that reads by judicial construction what Congress quite plainly rejected, a Fourth-Amendment-like rule that the suppression rule does not apply when "the government played no part in the unlawful interception." United States v. Murdock, 63 F.3d 1391, 1404 (6th Cir. 1995). The

suppression remedy to any violation either by the government or a private party of any of the surveillance statutes, both in the case of content and non-content information.

The second and related question considers whether to combine the suppression remedy with deferential doctrines to limit instances of suppression while nonetheless allowing the court to apply the law to the facts. Fourth Amendment jurisprudence contains a host of such doctrines. For example, under the good faith exception announced in *United States v. Leon*,[155] a court will not suppress evidence "seized in reasonable, good-faith reliance on a search warrant that is subsequently held to be defective."[156] Similarly, under the inevitable discovery doctrine announced in *Nix v. Williams*,[157] courts will not suppress evidence obtained in violation of the Fourth Amendment if the police can "establish by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means."[158] Finally, under the apparent authority doctrine announced in *Illinois v. Rodriguez*,[159] courts will not suppress evidence obtained in reliance on the consent of a third party to a search, even if the third party did not have the authority to consent, if based on "the facts available to the officer at the moment . . . a man of reasonable caution [would believe] that the consenting party had authority"[160] to consent. All three of these exceptions act as safety valves. They allow the courts to pronounce the law by applying it to the facts, but then avoid suppression of evidence unless the violation is particularly clear or egregious.

Any statutory suppression remedy for violations of the Internet surveillance laws would have to address both sets of these questions. Consider the current telephone surveillance law. The law extends the suppression remedy only to violations of the Wiretap Act, not the Pen

Court reasoned that punishing the government for the illegal act of a private citizen makes little sense, in part because it would not deter government misconduct. *Id.* This is clearly Congress' decision to make, however, and Congress chose to expand the suppression remedy to both private and government acts. *See In re* Grand Jury, 111 F.3d 1066, 1077–78 (3d Cir. 1997) (rejecting *Murdock*). This is a sensible decision on Congress' part. If the suppression remedy applies only to government misconduct, a private party can make an illegal surreptitious interception of another person's phone call, send it in to the police anonymously, and allow the government to use the evidence against the party whose communication was illegally intercepted. The Fourth Amendment would allow such a result under the private search doctrine, *see Kennedy*, 81 F. Supp. 2d at 1110, but Congress could reasonably conclude that greater privacy protection is required in the context of the Wiretap Act.

155. 468 U.S. 897.

156. *Id.* at 905.

157. 467 U.S. 431 (1984).

158. *Id.* at 444.

159. 497 U.S. 177 (1990).

160. *Id.* at 188–89.

Register statute or Stored Communications Act, and also allows violations by both state actors and private actors to trigger suppression.[161] At the same time, when the government obtains a Title III order that is later proved to be defective, the court will suppress the evidence only if the defect was important;[162] mere technical errors will not trigger suppression.[163] Notably, all three surveillance statutes also contain "good faith" defenses stating that good faith reliance on a "legislative authorization" or "statutory authorization" provides a complete defense to a civil or criminal action.[164] These defenses do not appear to apply in the context of a suppression hearing, however, and in any event cases construing them have been notably erratic.[165]

Rather than select one specific proposal for Congress, I will make two guiding observations instead. First, the answers to the two questions are necessarily linked. The broader Congress sees fit to extend the suppression remedy, the more need arises for doctrines to temper the broad rule. Conversely, if Congress opts for a robust set of safety valve defenses, it can match that with a broader suppression rule than otherwise. Second, I think a well-designed set of safety valve defenses would likely improve the implementation of a suppression remedy in the early stages of its existence. For example, a safety valve modeled after the qualified immunity doctrine would enforce the suppression rule when the law is clearly violated but not when the law remains vague.[166] This would serve the interests of law enforcement and civil libertarians alike. On one hand, it would satisfy law enforcement by allowing evidence to be used when the

161. *See* CCIPS Manual, *supra* note 3, at ch. 3–4.

162. United States v. Giordano, 416 U.S. 505, 527 (1974) (limiting suppression to cases in which defective order "fail[ed] to satisfy any of those statutory requirements that directly and substantially implement the congressional intention [in enacting Title III] to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative advice.").

163. *See, e.g.*, United States v. Moore, 41 F.3d 370, 375 (8th Cir. 1994) (reversing district court's suppression order on ground that judge's failure to sign the Title III order in the correct place was merely a technical defect).

164. 18 U.S.C. §§ 2520(d)(1), 3123(e) (1993); 2707(e)(1) (Supp. 2002).

165. *See* CCIPS Manual, *supra* note 3, at 177–78 (summarizing cases).

166. Under the doctrine of qualified immunity, "government officials performing discretionary functions, generally are shielded from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known." Harlow v. Fitzgerald, 457 U.S. 800, 818 (1982). In general, qualified immunity protects government officials from civil suit when "[t]he contours of the right" violated were not so clear that a reasonable person would understand that his conduct violated the law. Anderson v. Creighton, 483 U.S. 635, 640 (1987). When there is a "dearth of law surrounding the . . . statute" the absence of case law can help trigger qualified immunity. Blake v. Wright, 179 F.3d 1003, 1013 (6th Cir. 1999) (applying qualified immunity doctrine to the Wiretap Act).

government's "error" is merely a disagreement with the court over a difficult question of law. On the other hand, such a rule would further civil liberties interests in the long run by allowing the courts to clarify the law for future cases without the pervasive bias of suppression influencing the courts to rule in favor of law enforcement claims.

B. Why Civil Liberties Groups Should Support the Proposal

The case for why civil liberties groups should support my proposal is an easy one to make. Adding a suppression remedy to the Internet surveillance laws has been a goal among civil liberties groups since the laws were passed in 1986.[167] For the most part, the civil liberties argument has been framed for the public in terms of the enforceability of the surveillance laws. By adding a suppression remedy, the argument runs, law enforcement will finally have a reason to comply with the law. The remedy will give the law a much-needed "bite."[168]

Beyond enforceability, however, the addition of a statutory suppression remedy would have other major benefits from the standpoint of civil liberties. First and foremost, the change would finally expose the government's Internet surveillance practices to judicial scrutiny, and as a result, to public scrutiny. The suppression remedy would lift the "fog" of Internet surveillance, as defendants would bring challenges to the government's practices in court, and judges would be required to resolve whether the government's practices complied with the laws Congress passed to regulate it. Those resolutions would form part of the public record, creating a body of judicial precedents available to the public explaining exactly what the government can and can't do. Where the laws grant the government substantial powers, courts would decide cases saying so, creating a public record of the government's power which could provide a catalyst for legislative change curtailing the government's powers.

On a related note, a suppression remedy would expose and focus attention on specific instances in which the government may have violated the rules. Under current law, the government's Internet surveillance practices rarely become public, stoking fears of government abuse. A suppression remedy would restore a sense of

167. *See, e.g.*, *The Fourth Amendment and the Internet: Hearing Before the Subcommittee on the Constitution of the House Judiciary Committee*, 106th Cong. 25 (2002) (statement of James X. Dempsey, recommending that Congress add electronic communications to the Title III exclusionary rule in 18 U.S.C. § 2515 and add a similar rule to the § 2703 authority), *available at* http://www.house.gov/judiciary/demp0406.htm.

168. *See* Leib, *supra* note 11.

accountability to the government's Internet surveillance practices and replace general anxiety about Big Brother online with a more focused attention on actual instances of misconduct.

C. Why the Justice Department Should Support the Proposal

Convincing the Justice Department to support a proposal adding a suppression remedy is the tougher challenge. After all, the DOJ successfully fought off such a remedy in 1986.[169] Why would DOJ want to make life harder for its prosecutors, giving defense attorneys a new tool to try to have evidence thrown out in court, potentially resulting in the loss of important criminal cases and the resulting harm to public safety? This section argues that DOJ should want just such a rule, at least when tempered by safety valves such as good faith defenses that will minimize actual instance of suppression when violations of rules are merely technical or hinge on debatable questions of law.

DOJ should want such a rule for several reasons. First, judicial clarification of the law would serve DOJ's interests. As the Supreme Court has noted in the Fourth Amendment context, law enforcement works best when the government law provides clear and readily administrable rules for the government to follow.[170] Under the current remedies regime, the lack of clarity in the law may exert a chilling effect on investigative practices. Faced with legal uncertainty and little prospect of judicial clarification, the government may adopt interpretations of the law internally that are significantly more restrictive than a court would allow. If courts began to step in and draw clear boundaries, however, the existence of clear lines would free law enforcement to confidently exercise its powers within the boundaries drawn by the courts.

Second, the addition of a suppression remedy would give DOJ a considerable amount of control over the forum and context of the surveillance disputes the courts resolve, as well as the arguments the courts hear. Currently, the courts encounter Internet surveillance disputes mostly in civil cases between private parties, such as *Doubleclick* and *Konop*. DOJ ordinarily does not know about such

169. *See* Leib, *supra* note 11.

170. *See* Atwater v. Lago Vista, 532 U.S. 318 (2001).

> Often enough, the Fourth Amendment has to be applied on the spur (and in the heat) of the moment, and the object in implementing its command of reasonableness is to draw standards sufficiently clear and simple to be applied with a fair prospect of surviving judicial second-guessing months and years after an arrest or search is made. Courts attempting to strike a reasonable Fourth Amendment balance thus credit the government's side with an essential interest in readily administrable rules.

Id. at 347.

disputes until the decisions they produce are published, and has no opportunity to offer its own interpretation of the primarily criminal laws at issue.[171] In contrast, DOJ will be a party to every federal criminal case, and therefore will have a full opportunity to offer its views on the law. DOJ can also exercise significant control over the courts' docket in criminal cases. If a case raises difficult surveillance issues that the DOJ does not want a court to resolve given the facts of the case, DOJ can either refuse to indict the case, or else can move to dismiss its indictment or enter into a sweetheart plea agreement to moot a defense challenge. The fact that a federal prosecutor cannot appeal an adverse ruling without pre-approval from the Solicitor General's Office would further add to the effectiveness of DOJ's control of the docket if a statutory suppression remedy existed.[172] If a district court judge ruled against the government and suppressed evidence on the grounds that the government violated the surveillance laws, attorneys in the Solicitor General's Office would determine whether it would be in law enforcement's best interests to seek appellate review (triggering an appellate opinion instead of a district court order).[173]

Third, litigating Internet surveillance law in criminal cases would provide the government with a sympathetic forum in which to press its arguments. As noted earlier, criminal cases raise different stakes than civil cases, and courts may be more inclined to rule against criminal defendants than civil plaintiffs. This dynamic has received some attention in the scholarship on Fourth Amendment law. Akhil Amar and others have criticized the exclusionary rule for causing Fourth Amendment issues to arise primarily in criminal cases, where

171. In the case of *Konop*, for example, DOJ was unaware of the case until the Ninth Circuit's published opinion appeared on Westlaw. *See* Liu, *supra* note 145, at B1. At that point, DOJ was able to file an *amicus curiae* brief in favor of the Hawaiian Airlines petition for rehearing. However, if Hawaiian Airlines had opted not to pursue review of the panel's decision, DOJ would have had no opportunity to intervene in the dispute and help the courts understand the error of the court's approach in *Konop I*.

172. *See* Margaret Meriwether Cordray & Richard Cordray, *The Supreme Court's Plenary Docket*, 58 WASH. & LEE L. REV. 737, 766 (2001).

> By law, the federal government cannot appeal an adverse decision by a district court or a circuit court without the approval of the Solicitor General"); 28 C.F.R. § 0.20 (2000) ("The following-described matters are assigned to, and shall be conducted, handled, or supervised by, the Solicitor General, in consultation with each agency or official concerned .... (b) Determining whether, and to what extent, appeals will be taken by the Government to all appellate courts (including petitions for rehearing en banc and petitions to such courts for the issuance of extraordinary writs) and ... (c) Determining whether a brief amicus curiae will be filed by the Government, or whether the Government will intervene, in any appellate court.

Id.

173. *See* 28 C.F.R. § 0.20 (2000).

courts may construe the government's powers broadly to avoid letting a criminal go free.[174] Applying this insight in reverse, the government should want the rules governing it to be decided by the courts in criminal cases. By causing questions of Internet surveillance law to arise in criminal cases, a suppression remedy will result in judicial resolution of ambiguous laws in a sympathetic context for the government.

The fourth reason DOJ should want a suppression remedy is that public understanding of surveillance law would likely lead to more public support for law enforcement online, rather than less. Today's press is quite enamored with visions of the government online as an omnipresent Big Brother. As a result, the media tends to overreport the amount of power law enforcement has online and tends to underreport the amount of privacy Internet users enjoy. This misreporting occurs at least in part because limitations on the government's power that are acutely felt within the government remain unknown outside the government. The fog of Internet surveillance law keeps the press and the public unaware of the limitations the government faces investigating routine criminal cases. A suppression remedy would change that. By triggering criminal cases interpreting the surveillance laws, a suppression remedy would show the public how the surveillance laws regulate and restrict the government as it tries to pursue hackers, pedophiles, fraudsters and terrorists online. Cases construing the government's powers would reveal the limits of the government's powers, fostering a political climate more sympathetic to the government's position than the current one.

Conclusion

The Supreme Court's interpretation of the Fourth Amendment has left Internet surveillance law to develop as a primarily statutory field. As a result, the rules that regulate the people's government are

174. *See, e.g.* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 799 (1994) (arguing that judges distort Fourth Amendment doctrine to find no violation in sympathetic criminal cases); George C. Thomas, III & Barry S. Pollack, *Saving Rights from a Remedy: A Societal View of the Fourth Amendment*, 73 B.U. L. REV. 147, 168 (1993) ("If the only option when finding a violation is to suppress the evidence, judges may feel themselves hemmed in by the doctrine and may define the Fourth Amendment as necessary on a case-by-case basis to permit the use of seized evidence."); David Moran, *The New Fourth Amendment Vehicle Doctrine: Stop and Search Any Car at Any Time*, 47 VILL. L. REV. 815, 815 (2002) (noting that "[s]everal commentators have argued that the exclusionary rule has harmed Fourth Amendment values because judges are more likely to give the Fourth Amendment a grudging and narrow interpretation when a criminal defendant seeks to exclude probative evidence of her guilt than when a civil litigant seeks damages.").

up to the people and the legislators they elect to represent them. I think this arrangement has the potential to lead to an optimal set of rules governing law enforcement, a set of rules far better than those that would result if the courts alone tried to set up the rules under the guise of the Fourth Amendment. The public's tremendous interest in and concern about Internet privacy, combined with its recognition of the importance of allowing the government to investigate crimes, can lead to a balanced and thoughtful set of rules that protect both privacy and public safety.

For the legislative process to work, however, the law must provide a feedback loop. The law must generate cases that tell Congress and the public how the law is working in practice. The feedback loop can then allow Congress and the public to enact changes that tweak the rules to strike a better balance between privacy and security. In some cases, the changes will restrict law enforcement powers; in others, they will expand the powers. In both cases, however, the feedback loop acts as an essential control on the legislative process. It guarantees that the laws the people want are the laws the people get.

By choosing to enforce the laws though civil remedies rather than an exclusionary rule, Congress has inadvertently cut the feedback loop of Internet surveillance law. The absence of criminal cases and existence of a few aberrant civil cases has created a statutory fog. Few understand how the law works, few understand the limits of the government's power, and the government itself lacks clear rules allowing it to exercise its powers. Congress no doubt meant well when it agreed to limit the remedies to the civil context in 1986. Legislators presumably believed that civil remedies would ensure that the laws were enforced without punishing the government with a loss of evidence if a court ruled that the government violated the rules. This choice has had an unintended consequence, however: by shielding the government's conduct from judicial scrutiny in routine criminal cases, the remedies scheme blocked the courts from being able to explain how the law applied, which both blocked the law from developing in the courts, and shielded Congress, the press, and the public from a clear vision of how the laws work in the field.

As Justice Brandeis famously noted, "[s]unlight is said to be the best of disinfectants."[175] Sixteen years after ECPA passed, it is now clear that Congress's remedies scheme has served neither the interests of the DOJ that proposed the scheme, nor the civil

175. LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY, AND HOW THE BANKERS USE IT 92 (1914) ("Sunlight is said to be the best of disinfectants; electric light the most efficient policeman."), *reprinted in* THE WORDS OF JUSTICE BRANDEIS 158 (Solomon Goldman ed., 1953).

libertarians who opposed it. The law remains in a fog. Congress should reconsider its 1986 decision and add a statutory suppression remedy. Shedding light on the surveillance laws will illuminate the law to everyone's benefit.

***